REVIEW OF THE SMALL BUSINESS ADMINISTRATION'S PROTECTION OF SENSITIVE AGENCY INFORMATION

Report Number: 07-13
Date Issued: February 9, 2007

Memorandum

U.S. Small Business Administration
Office of Inspector General

To: Christine Liu
Chief Information Officer
Chief Privacy Officer

Date: February 9, 2007

From: **/S/ Original Signed**
Debra S. Ritt
Assistant Inspector General for Auditing

Subject: Advisory Memorandum Report on SBA's Protection of Sensitive Agency Information

Following numerous incidents involving the compromise or loss of sensitive personal information, on June 23, 2006, the Office of Management and Budget (OMB) issued Memorandum 06-16 *Protection of Sensitive Agency Information,*[1] requiring federal agencies to take certain actions to protect sensitive information entrusted to them. These actions, which were to be implemented by August 7, 2006, included: (1) encrypting mobile computers and storage devices; (2) implementing remote two-factor authentication for access to internal government networks; (3) installing time-out features when logged into internal government networks; and (4) maintaining logs of sensitive information stored on mobile computers. The memorandum also directed the OIGs to review agency progress in implementing safeguards.

As required, we evaluated SBA's progress in implementing actions directed by OMB to protect sensitive agency information. We reviewed the Agency's policies and procedures on information security and privacy, interviewed responsible systems security personnel in the Office of Chief Information Officer, and

[1] Sensitive information is any information, the loss, misuse, or unauthorized access to or modification of, which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.

conducted a limited test of SBA's Virtual Private Network to determine the adequacy of user reauthenticaton requirements. Our evaluation was performed at SBA's headquarters during August and September 2006, and our report was issued on September 22, 2006.

Since that time we have performed additional work to assess the current status of SBA efforts. This report presents additional details supporting our earlier findings, provides the status of SBA's data protection activities as of December 1, 2006, and makes five recommendations to further strengthen safeguards to protect sensitive agency information.

RESULTS IN BRIEF

Information Redacted **[Exemption 2]**

SBA reviewed a draft of this report and concurred with the findings and recommendations. SBA's full response is included in Appendix I of this report.

FINDINGS

SBA Has Not Encrypted Sensitive Data on Mobile Computers and Devices

OMB Memorandum 06-16 requires encryption for all data on mobile computers/devices, which carry Agency data unless the data is determined to be non-sensitive. However, as of August 7, 2006, SBA did not have a full inventory of information systems that contained personally identifiable information. At the time of our review, SBA had adequately assessed 20 out of a potential 101 systems for sensitive information.

Information Redacted **[Exemption 2]**

SBA Had Not Implemented a Remote Two-Factor Authentication for Accessing the Agency Network

OMB Memorandum 06-16 requires that remote access to a network only be allowed when a device separate from the computer gaining access is used.

Information Redacted **[Exemption 2]**

SBA Does Not Have a "Time-Out" Function For Email Remote Access

OMB requires that a "time-out" function be employed for remote access and mobile devices that relies on user reauthentication after 30 minutes of inactivity.

Information Redacted **[Exemption 2]**

Logs of Computer-Readable Data Extracts Are Not Maintained

As of August 7, 2006, SBA did not have logs of computer-readable data extracts from systems containing sensitive information. OMB Memorandum 06-16 requires Agencies to log all computer-readable data extracts from databases holding sensitive information and to verify that each extract including sensitive data has been erased within 90 days, unless its use is still required. Our evaluation disclosed that SBA did not have procedures to create such logs or procedures to ensure the erasure of old unneeded data extracts.

As of December 1, 2006, SBA determined that some of its offices had created computer-readable data extracts of sensitive information used by employees and contractors. Additionally, SBA is planning to write the necessary procedures to require that a record be maintained of data extracts from sensitive Agency databases and that those extracts are erased when they are no longer needed. Until SBA completes these activities, it will not have a record of the sensitive data stored in each of its systems needed to properly respond to incidents involving the loss or compromise of sensitive data.

RECOMMENDATIONS

We recommend that the Chief Information Officer:

1. Complete an inventory of information systems containing sensitive Agency information.

2. *Information Redacted.* **[Exemption 2]**

3. *Information Redacted.* **[Exemption 2]**

4. *Information Redacted.* **[Exemption 2]**

5. Log all computer-readable data extracts from databases holding sensitive information and verify that each extract including sensitive data has been erased within 90 days unless further needed.

AGENCY COMMENTS

The Agency provided written comments concurring with all findings and recommendations in the draft report. SBA's comments are summarized in the Results in Brief section, and the full text of the comments can be found in Appendix I to this report.

APPENDIX I. SCOPE AND METHODOLOGY

As required by OMB, we evaluated SBA's progress in implementing of Memorandum 06-16 as of August 7, 2006. We used a "data collection instrument" developed by the President's Council on Integrity and Efficiency to answer specific questions regarding the implementation of Memorandum 06-16.

We also interviewed SBA's information systems security officer and other personnel responsible for managing SBA's implementation of Memorandum 06-16 requirements. We examined SBA's policy and procedures relative to information security and privacy. We also conducted a functional test on SBA's Virtual Private Network (VPN) to determine whether it required user re-authentication after 30 minutes of inactivity.

Our initial evaluation was performed at SBA's headquarters office in Washington, D.C. during August and September 2006, and we submitted the completed data collection instrument to the Office of Inspector General, Department of Education on September 22, 2006. We obtained additional status updates regarding SBA's efforts in this area through December 1, 2006.

APPENDIX II. MANAGEMENT COMMENTS

U.S. SMALL BUSINESS ADMINISTRATION
WASHINGTON, DC 20416

Date: January 25, 2007

To: Debra S. Ritt
Assistant Inspector General for Auditing

/S/ Original Signed
From: Christine H. Liu
Chief Information Officer
Chief Privacy Officer

Subject: OCIO's Response to Draft Advisory Memorandum Report on SBA's Protection of Sensitive Agency Information

Please find attached OCIO's response to the recommendations addressed in the above report. If you require additional information, please contact me at (202) 205 **[Exemption 2]**

Attachment

cc: Jovita Carranza
Deputy Administrator

Response to Office of Inspector General's Audit Report on the Review of the Small Business Administration's Protection of Sensitive Agency Information (Project No. 6028):

OIG's Recommendations

1. **Complete an inventory of information systems containing sensitive Agency information. (Agree)**

   OCIO's Response: OCIO completed an inventory of the Agency's major and minor information systems containing sensitive information. Privacy Impact Assessments (PIAs) for the Agency's major information systems will be completed 1/31/07 and PIAs for the minor systems are scheduled for completion 2/28/07.

2. ***Information Redacted.*** **[Exemption 2]**

3. ***Information Redacted.*** **[Exemption 2]**

4. ***Information Redacted.*** **[Exemption 2]**

5. **Log all computer-readable data extracts from databases holding sensitive information and verify that each extract including sensitive data has been erased within 90 days unless further needed. (Agree)**

   OCIO's Response: SOP 90-47 "Automated Information Security Program" is currently under revision to address this recommendation.

APPENDIX III. REPORT DISTRIBUTION

Recipient	No. of Copies
Office of the Chief Financial Officer Attention: Jeffrey Brown	1
General Counsel	3
Office of Management and Budget	1
U.S. Government Accountability Office	1